PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G07F 7/10

A1

(11) International Publication Number: **WO 98/59327**

(43) International Publication Date: 30 December 1998 (30.12.98)

(21) International Application Number: PCT/SE98/01019

(22) International Filing Date: 28 May 1998 (28.05.98)

(30) Priority Data:
9702216-4 10 June 1997 (10.06.97) SE

(71) Applicant *(for all designated States except US)*: DIGITAL EQUIPMENT BCFI AB [SE/SE]; P.O. Box 904, S-175 29 Järfälla (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: HEDIN, Bengt [SE/SE]; Citronvägen 6, S-175 49 Järfälla (SE). JANSSON, Kjell [SE/SE]; Backvägen 6, S-194 44 Upplands Väsby (SE). MOLANDER, Bo [SE/SE]; Tavastgatan 7, S-118 24 Stockholm (SE).

(74) Agent: AWAPATENT AB; P.O. Box 45086, S-104 30 Stockholm (SE).

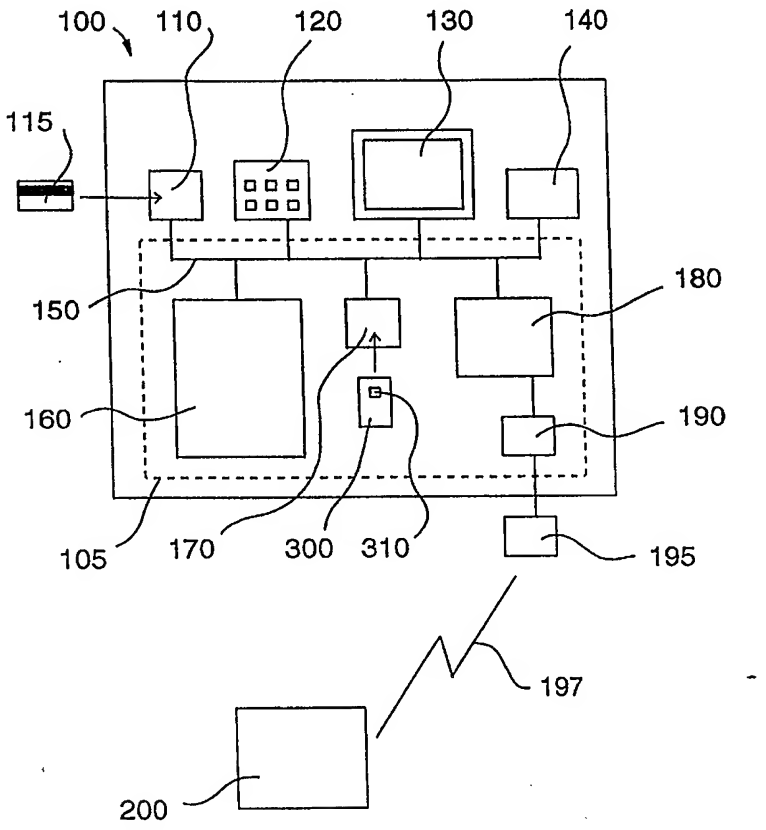
(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
In English translation (filed in Swedish).

(54) Title: SAFETY MODULE

(57) Abstract

The present invention relates to an IC card, a transaction station as well as uses thereof. According to the invention, a cryptographic IC card, which is essentially stationarily arranged in a card reader in connection with a transaction station, such as an ATM or the like, is utilised for cryptographic processing of data which is to be transmitted between the transaction station and a central computer. The IC card replaces conventional safety modules and is thus arranged essentially stationarily in the card reader and is consequently used in connection with the serving of several different users of the transaction station.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SAFETY MODULE

Technical Field

The present invention relates to cryptographic processing of the communication between a transaction station and a central computer in connection with financial transactions.

Background of the Invention and Prior Art

Presently, there are various examples of systems where different users or visitors utilise a transaction station, which is in communication with a central computer, for carrying out various types of financial transactions through the central computer.

So-called ATMs (Automatic Teller Machines) are probably the most common example of such transaction stations. With the aid of an ATM, a customer in a bank or a like user can withdraw money from his own bank account or carry out similar financial transactions. Usually, the user identifies himself with the aid of a magnetic card or the like, which is read by a card reader in the ATM and thus provides the ATM with information about the user's account number, bank, or the like. Subsequently, the user confirms that he is an authorised user of the card, i.e. the account, by entering a so-called PIN code (PIN - Personal Identification Number), which usually consists of a combination of four numbers and which is known only by the cardholder (user). The PIN code is usually entered with the aid of a keypad located on the ATM. Subsequently, the user indicates the transaction he wishes to carry out, usually a desired withdrawal amount. Next, the ATM transmits this information (account number, PIN code, withdrawal amount) to a central computer which contains information about the accounts of various cardholders. The communication between the ATM and the central computer often takes place by the intermediary of a

telephone connection. The central computer verifies that the PIN code entered is the correct one for the account number provided and, if so, transmits an enabling signal to the ATM, which enabling signal indicates that the transaction has been approved. Upon receipt of the approval, the ATM dispenses notes corresponding to the desired withdrawal amount from a note dispenser to the user. If the central computer determines that the PIN code entered is incorrect for the account number provided, it transmits an error signal to the ATM, in which case the latter either allows the user to make another attempt to enter the correct PIN code, returns the card to the user without dispensing any cash, or withholds the card. In some cases, the verification of the PIN code and the like can also take place in the transaction station itself, so-called off-line verification.

In connection with the transmission of transaction messages of the above kind between the transaction station and the central computer, it is necessary or desirable for at least certain types of information to be transmitted in encrypted form and for the messages to be provided with authentication in the form of MAC sums (Message Authentication Codes) or the like. This ensures both that the information cannot be accessed or listened in on by unauthorised individuals and that messages received have not been distorted or altered during the transmission.

In order to provide the above-mentioned and similar cryptographic functions, such as encrypting, decrypting, authentication, etc., transaction stations are equipped with a so-called safety module, in which cryptographic keys and algorithms for the communication between the transaction station and the central computer are provided and executed. The safety module is essentially fixedly or stationarily connected to the transaction station. In the case of ATMs, the safety module is generally fixedly connected inside a safety cabinet in the machine.

Since one wishes to ensure that unauthorised individuals do not gain access to the information in the safety module, i.e. primarily the cryptographic keys, the safety module is protected by embedding the electronic circuitry inside a physically protective shell and by providing the module with a destruct function which, by utilising various sensor members, e.g. an enclosing metal layer, is intended to destroy the cryptographic keys and other essential software in the event that someone tries to break open the safety module.

Moreover, the safety module is usually equipped with a battery which ensures that the cryptographic keys are retained in the memory even if the power supply to the safety module is temporarily cut off or is lacking, for example in connection with a power cut or when an ATM is temporarily shut off for maintenance, repairs, updating or the like. The battery is also active from the time when the safety module is provided with the cryptographic keys until the safety module has been arranged inside or adjacent to the transaction station and the latter has been connected to mains current. In some cases, the battery may also be necessary for maintaining the above-mentioned destruct function in a situation where the safety module has been disconnected.

A problem associated with these types of safety modules is that the need to protect the contents from unauthorised access, and therefore the necessity of safety arrangements and destruct functions, results in additional difficulties and costs in connection with the manufacture and design of the safety module.

Another problem is that the battery which is usually required exhibits a limited guaranteed functional life, e.g. 5 years, whether it be rechargeable or not. This means that the safety module, or the battery therein, must be replaced at regular intervals, which is not an entirely uncomplicated process in the case of many types of safety modules. Consequently, this puts demands on the

manufacturer's service organisation. It also means that there are limited possibilities for stocking safety modules. In addition, used batteries must be disposed of, something which must be carried out according to proper environmental procedures.

A further problem is that a malfunction of the safety module cannot be easily dealt with. Often, service staff must go to the malfunctioning transaction station to replace or repair the malfunctioning part of the safety module. Naturally, this results in undesired costs and time periods when the transaction station is not usable.

It is thus an object of the present invention to provide a simpler solution which reduces the risk of unauthorised individuals reading the contents of the safety module, primarily the cryptographic keys.

Another object of the invention is to provide a solution which avoids the problems connected with the limited life of the battery.

Yet another object is to provide a solution which enables easier and quicker repair, maintenance and updating of the safety module.

Summary of the Invention

According to a first aspect of the present invention, the above-mentioned as well as other objects are achieved by an IC card designed to be essentially stationarily arranged in a card reader inside, or adjacent to, a transaction station for cryptographic processing of data which is to be transmitted from the transaction station to a central computer and/or data which is received by the transaction station from a central computer, said IC card being utilised in connection with the serving of several different users of said transaction station, which IC card comprises: means for storing one or more cryptographic keys; means for receiving input signals to the card; means for executing one or more cryptographic algorithms utilising one or more of said cryptographic

keys depending on the control information received in said input signals to the card; and means for outputting output signals, comprising the result of said execution, from the card.

The invention is thus based upon the idea of replacing the conventional safety module with an IC card reader provided with an IC card according to the invention, which supplies the keys and algorithms required for cryptographic processing of the communication between the transaction station and the central computer.

According to preferred embodiments, the IC card is utilised for e.g. encryption, decryption and authentication of messages. Accordingly, the IC card advantageously stores master keys as well as session keys and authentication keys. The preferred algorithm for cryptographic processing is the so-called DES algorithm (DES - Data Encryption Standard).

An inherent advantageous characteristic of IC cards is that their physical structure is such that cryptographic keys stored therein normally cannot be read from the card, considering what is practicable using existing technology. Consequently, the utilisation of an IC card according to the invention, as a replacement for the conventional safety module, results in inherent protection against the risk of an unauthorised individual gaining access to the secret keys. Even if the IC card itself were to fall into the wrong hands, this individual will still not gain access to the keys. Consequently, the IC cards themselves can be handled without any special safety arrangements. If an IC card were to malfunction in a transaction station, a new card could easily be sent by mail to the persons responsible for the ongoing operation of the transaction station. Moreover, service staff responsible for maintenance of transaction stations would not need to take pains to employ special safety arrangements for safekeeping the IC cards; in principle the cards could be handled in the same manner as other compo-

nents of the device. However, it should be noted that according to a possible embodiment, the invention is not restricted to the non-readability of the keys from the card, although, in practice, this is a very essential feature.

Since, according to a preferred embodiment, the memory used in the IC card consists of a non-volatile memory, usually of the EEPROM type, in which the information in the memory cells is changed with the aid of electrical signals but is physically preserved without any holding current being required, the need for providing a separate auxiliary current feed for the memory part of the IC card is eliminated, which is an advantageous difference in comparison with the known safety module. Nor is a current feed required for maintaining an active safety function in the card when it is not located in the card reader, in comparison with the conventional safety module, since there is an inherent safety function in the structure of the IC card, as discussed above.

IC cards according to the invention are not restricted to a specific card size. Accordingly, different embodiments of the invention comprise, for example, IC cards of the following size types: ID-1, ID-00 (mini-cards), and ID-000 (plug-in cards).

In this connection, it should be noted that the IC card according to the invention should not be equated with the various types of cards, such as magnetic cards or IC cards, which a user of a transaction station sometimes carries to gain access to and utilise the station, such as ATM cards, credit cards or the like normally issued for personal use. Those types of cards are utilised only very temporarily in the transaction station when the specific cardholder is being served. Instead, the IC card according to the invention is intended to be generally stationarily arranged in, or adjacent to, the transaction station. The IC card according to the invention is thus utilised essentially continuously in the

transaction station in connection with the serving of several different users visiting the transaction station, usually one at a time.

Furthermore, it will be appreciated that the term generally stationarily means that the IC card according to the invention is permanently arranged in the transaction station during on-going operation, but that, obviously, the card can be replaced when required, for example in connection with a malfunction, when replacing or updating keys, or at regular intervals as a pure upgrading measure.

According to a second aspect of the present invention, the invention relates to a transaction station, intended to communicate with a central computer and to serve a user in connection with the carrying out of desired financial transactions through the central computer, which transaction station comprises: a user interface for data inputting by a user; and means for cryptographic processing of data which is to be transmitted to and/or be received from the central computer; the transaction station according to the invention being characterised in that said means for cryptographic processing comprise a card reader intended to receive an IC card according to the above-mentioned first aspect of the present invention.

According to a particularly preferred embodiment, the transaction station according to the invention consists of an ATM ("Automatic Teller Machine"), for example of the types which in Sweden are provided in public places, in banks, etc., under the brand names "Bankomat" and "Minuten".

According to yet another preferred embodiment said card reader is adapted to receive said IC card in such a way that it is inaccessible to a user. This reduces the risk of a user deliberately or inadvertently removing the IC card according to the invention, something which is not of great importance from the point of view of safety,

as discussed above, but which nevertheless would mean that the encrypting function of the transaction station would be put out of order. One way of achieving this is for the transaction station to be designed in such a way that the user only has access to a certain interface, while the card reader for the IC card according to the invention does not form part of this interface but is instead located elsewhere. For example, according to a further preferred embodiment, said card reader for the IC card according to the invention is arranged in a safety cabinet, for example inside the transaction station or adjacent to the transaction station.

A user interface as stated above advantageously comprises means for inputting a user identity, such as an additional card reader for reading an account number which is magnetically stored in the user's credit card; means for inputting a desired financial transaction, such as a keypad, and means for inputting an access code, such as a PIN code. In this context, it should be noted that said additional card reader for reading, for example, an account number stored in the user's credit card does not constitute the same card reader as the one employed for receiving the IC card according to the invention. According to another alternative, the user interface comprises a personal computer with an associated monitor, keyboard, mouse or like pointing device.

The transaction station according to the invention advantageously comprises means for providing control information, such as information concerning the desired type of cryptographic processing as well as information or data required for this processing, to said IC card according to the invention, as well as means for receiving said output signals from the IC card.

Although ATMs constitute a preferred embodiment of the invention, a transaction station according to the invention can, for example, be designed as a so-called payment terminal which, for example, is located adjacent

to cash registers in supermarkets, shops, and the like, where the customer can pay for goods or services purchased by, for example, entering an account number, usually also by means of a magnetic card, and confirming that he is an authorised user by inputting the correct PIN code. According to one variant, one or more payment terminals are connected to a personal computer which in turn communicates with a central computer at a bank or the like.

A further example of transaction stations according to the invention comprise personal computer terminals which are configured to enable the user to request various financial transactions in a similar way through a central computer. Such personal computer terminals can, for example, be made available to the public in public places, in banks, in companies as a service offered to employees, or explicitly for the accounting functions of the company. The technique of providing this type of opportunity to carry out financial transactions at home with the aid of computers is also more or less a reality already.

Other types of financial transactions and functions can also be carried out by means of transaction stations according to the invention, such as transfers between different bank accounts, balance information, payment orders, securities transactions, etc. Depending on the application and the system in question, there are also many different possible ways of obtaining information from the user, e.g. by utilising magnetic cards, IC cards, keyboards or keypads, touch screens, etc.

In the case of payment terminals, personal computers and the like, the IC card reader according to an embodiment is connected to an external port thereto and consequently constitutes an external unit.

Further aspects, objects, advantages, and features with respect to the present invention will appear from the appended claims and the description below.

Brief Description of the Drawings

An embodiment of the present invention will now be described by way of example with reference to the accompanying drawings, in which:

Fig. 1 schematically shows a perspective view of a transaction station in the form of an ATM according to the present invention;

Fig. 2 is a schematic block diagram of the transaction station in Fig. 1;

Fig. 3 is a schematic block diagram of the integrated circuit on the IC card in Fig. 2;

Fig. 4 is a flowchart for the control computer in Fig. 2;

Fig. 5 shows the structure of an example of a message being transmitted from the transaction station to the central computer in Fig. 2; and

Fig. 6 is a flowchart for the integrated circuit in Fig. 3.

Detailed Description of a Preferred Embodiment

Fig. 1 is a perspective view of a transaction station 100 in the form of an ATM according to a preferred embodiment of the invention.

The transaction station 100 in Fig. 1 comprises a first card reader 110 (only the insertion slot is shown), a keypad 120, a monitor 130, and a printer 140 (only the output slot is shown) The transaction station further comprises a note box with a note dispenser 160. The note box, together with other electronic circuitry which is preferably kept at a higher level of safety, see Fig. 2 below, is contained in a safety cabinet 105 of the transaction station.

Fig. 2 is a schematic block diagram of the transaction station in Fig. 1. The parts and components in Fig. 1 which are also shown in Fig. 2 are referred to by the same reference numerals. Thus, Fig. 2 shows the transaction station 100 comprising the card reader 110,

the keypad 120, the monitor 130, and the printer 140, all of which are arranged in an upper space in the transaction station 100. According to this embodiment, the card reader 110 is designed to receive and read a magnetic card 115 which the visitor or user, i.e. the cardholder, brings with him.

Moreover, the transaction station 100 comprises a note box 160, a safety module in the form of a second card reader 170 in which an IC card 300 exhibiting an integrated circuit 310 is arranged, a control computer 180 and a communication unit 190. Since extra high access protection is desired for these types of components, they are arranged in the safety cabinet 105 in the lower space of the transaction station 100.

The operation of the transaction station 100 is generally controlled by the control computer 180, which communicates with the first card reader 110, the keypad 120, the monitor 130, the printer 140, the note box/dispenser 160, and the second card reader 170 by the intermediary of a shared communication bus 150. With the aid of a modem 195, the transaction computer can be connected to a telephone network 197 and can thus communicate with a central computer 200 from a distance.

The integrated circuit 310 on the IC card 300, which in itself or together with the second card reader 170 can be said to form a safety module for the transaction station 100, provides the cryptographic algorithms and keys utilised in connection with the transmission of messages between the transaction station 100 and the central computer 200.

Examples of operational routines for the transaction computer in Figs 1 and 2 will be described below with reference to Figs 4, 5, and 6.

Fig. 3 is a schematic block diagram of the integrated circuit 310 of the IC card 300. The circuit 310 is thus formed on the IC card with the aid of conventional technology and can communicate with the control computer

180 when the IC card 300 is inserted into the second card reader 300.

The basic structure of the IC card 300 and the integrated circuit 310, such as connections and arrangements for transferring data between the card reader 170 and the integrated circuit 310 and like functions, are well known in the technical field relating to IC cards and, consequently, a more detailed description thereof will not be provided in this application.

The integrated circuit 310 of the IC card 300 generally comprises a microprocessor 315 and a non-volatile, writable memory 320, 330, usually of the EEPROM type.

The EEPROM memory comprises, inter alia, a first set of memory fields 320 which store the cryptographic keys employed in connection with cryptographic processing of messages transmitted between the transaction station 100 and the central computer 200. Usually, there are three different types of cryptographic keys stored in the memory fields 320. First, so-called authentication keys which are used in connection with the authentication of messages, e.g. for calculating so-called message authentication codes ("MACs"), second, so-called session keys which are used in connection with encryption/decryption of PIN codes and other sensitive information transmitted between the transaction station and the central computer, and, third, one or more master keys which are used, inter alia, when new keys are transmitted, i.e. when old session or authentication keys are to be replaced by new keys by the intermediary of the telephone network 197. Obviously, the central computer 200 has access to such corresponding keys as are necessary for the central station to handle the cryptographically processed communication with the transaction station.

Furthermore, each memory field 320, i.e. each key, is associated with a corresponding field of a second set of memory fields 330. The memory fields 330 store information setting out the applications or functions for

which the associated key may be utilised, since each specific key may usually only be used for a certain type of cryptographic processing or for cryptographic processing of only a certain type of information.

The processing in the integrated circuit 310 is carried out in the microprocessor 315. The microprocessor 315 is configured to carry out various types of cryptographic processing by executing various program routines 340-370, which are schematically illustrated separated by dashed lines in Fig. 3, by employing various selected keys from the memory field 320. The program routines in the microprocessor comprise a receiving/addressing routine which is configured to receive control information from the transaction station, preferably from the control computer 180. Such control information comprises, for example, information about the type of cryptographic processing requested, the cryptographic key to be used, data which is to be processed, etc.

In the preferred embodiment, essentially all types of cryptographic processing are carried out with the aid of a DES algorithm (DES - "Data Encryption Standard") in a program routine 360. The DES algorithm in block 360 is thus used in the preferred embodiment in connection with encryption as well as decryption and authentication. Depending on the type of cryptographic processing desired, one of several different preparatory program routines 351-353 are used, which prepare and configure the information required in the subsequent DES algorithm 360 in order for the latter to provide the type of cryptographic processing desired. For example, the program routine 351 is addressed when encryption is requested, the program routine 352 when decryption is desired, and the program routine 353 when authentication is desired. In this connection, the respective program routine 351-353 fetches the keys to be utilised and structures the data to be processed in a suitable way, after which the actual cryptographic algorithm is carried out in the routine 360.

Furthermore, one or more subsequent program routines 370 are included which assemble the processed information in a suitable manner and feed it back to the control computer 180 of the transaction station by the intermediary of the card reader.

The person skilled in the art will appreciate that the operation and structure of the integrated circuit 310 and the microprocessor 315 can be readily implemented in many different ways and that the invention is not restricted to the program routines and memory fields described above by way of example. For example, the different program routines can be more or less integrated with one another. The actual program routines can be stored in a memory, similar to the way the information in the memory fields 320 and 330 is stored and, in this case, can be read into the microprocessor when requested. However, it is an important characteristic of the integrated circuit 310 that the cryptographic keys are stored in such a way that, in view of what is reasonable and technically possible, they cannot be read from the card and thereby become accessible to unauthorised individuals.

The microprocessor 315 can, for example, also comprise program routines which are executed in connection with the replacement or updating of keys, initialising of cards, etc.

An example of the mode of operation of the transaction station when serving a user or visitor will now be described with reference to Fig. 4, which schematically illustrates a flowchart for the control computer 180 in Fig. 2.

The routine shown in Fig. 4 is initiated in step S10 by the user inserting his magnetic card 115 into the card reader 110. In step S12, the card reader 110 reads the cardholder's account number, which is magnetically stored on the magnetic strip of the magnetic card 115, and feeds it to the control computer 180 by the intermediary of the

bus 150. In step S14, with the aid of the monitor 130, the control computer subsequently instructs the user to enter his PIN code with the aid of the keypad 120, after which the PIN code entered by the user is fed from the keypad 120 the control computer 180 by the intermediary of the bus 150. In step S16, with the aid of the monitor 130, the control computer 180 subsequently instructs the user to enter the desired withdrawal amount with the aid of the keypad 120, after which the amount entered by the user is fed from the keypad 120 to the control computer 180 by the intermediary of the bus 150.

Subsequent to obtaining the above information, the control computer sends an instruction, in step S18, to the IC card 310 which is essentially stationarily arranged in the transaction station and which constitutes the safety module of the transaction station, instructing it to carry out the encryption of the PIN code utilising a specified encryption key. Accordingly, in this case, the instruction to the IC card comprises control information in the form of details as to the operation requested (encryption), data which is to be processed (the PIN code entered), as well as details as to the key to be used for the processing. If desired, the account number, for example, could also be included in the information to be encrypted.

In step S20, when the IC card has returned the encrypted PIN code, the control computer puts together the account number of the user, the encrypted PIN code, and the amount requested into a single connected message.

Subsequently, in step S22, the control computer sends this message to the IC card 310 instructing it to calculate an authentication code (MAC) for the message. In this case, the instruction to the IC card thus comprises control information in the form of details as to the operation requested (calculation of authentication code), data to be processed (the message consisting of

the account number, the encrypted PIN code, and the amount), as well as details as to the key to be used.

Subsequently, the finished message is sent, e.g. by the intermediary of the telephone network 195, to the central computer 200 in step S24. An example of such a finished message is schematically shown in Fig. 5, in which the message comprises a first field 400 for the user's account number, a second field 410 for the encrypted PIN code, a third field 420 for the desired withdrawal amount 420, and a fourth field for the authentication code 430.

Next, in step 26, a reply is received from the central computer 200. In the case where the reply is expected to comprise an authentication code, the control computer instructs the IC card 300, step S28, to authenticate the reply message. Accordingly, in this case, the instruction to the IC card comprises control information in the form of details as to the operation requested (authentication), data to be processed (the reply message), as well as details as to the key to be used.

After step S28, if the result of the authentication in the IC card is that the reply message is incorrect for some reason, the control computer proceeds to a program routine which is not shown in Fig. 4, which may, for example, involve the transaction station 100 awaiting a new reply message from the central computer 200 or the transaction station 100 interrupting the current transaction and returning the magnetic card 115 to the user.

If the reply message from the central computer is correct, but states that the transaction requested is not approved, for example because the PIN code entered is incorrect or because the amount requested exceeds the balance available in the user's account, subsequent to step S28, the control computer 180 proceeds to a program routine which is not shown in Fig. 4, which, for example, may involve the transaction station 100 interrupting the current transaction and returning the magnetic card 115

to the user, the transaction station instructing the user to make a new attempt to enter the correct PIN code since the previous one was incorrect, or the transaction station withholding the user's magnetic card and interrupting the transaction without returning the card to the user.

However, if the reply message is authenticated as being correct and if, in addition, it contains a transaction approval, the transaction station 100, in step S30, dispenses the amount requested from the note box/dispenser 160 to the user, writes a transaction report to the user in the form of a transaction slip with the aid of the printer 140 in step S32, and returns the magnetic card 115 from the magnetic card reader to the user in step S34. Subsequently, in step S36, the transaction station returns to an idle position while waiting for a new magnetic card to be inserted into the card reader 110.

An example of the mode of operation of the IC card 300, i.e. the integrated circuit 310, in relation to the control computer 180 in the transaction station 100 will now be described with reference to Fig. 6, which shows a schematic flowchart for the microprocessor in Fig. 3.

The routine shown in Fig. 6 is initiated in steps B10 and B12 by the microprocessor 315, utilising the program routine 340 in Fig. 3, receiving an instruction by the intermediary of the bus 150 from the control computer 180 of the transaction station 100. The instruction may, for example, be the instruction sent from the control computer 180 to the IC card 300 in step S18 (request for encryption), step S22 (request for calculation of authentication code), or step S28 (request for authentication of reply) in the flowchart described with reference to Fig. 4 above.

Next, the microprocessor 315 establishes the type of function requested, i.e. the desired type of cryptographic processing, as well as the key to be used for this

function, in steps B14 and B16, respectively, by deriving this information from the instruction received. Subsequently, the microprocessor 315 verifies, in step B18, that the information in the field 330 associated with the memory field 320 for the key indicated states that the key may be utilised for the function requested. If not, the routine is interrupted and the IC card 300 informs the control computer 180 that the task will not be carried out.

Depending on the type of function to be carried out, this and similar kinds of preparatory obtaining, verifying, and formatting of information which is to be utilised in the actual cryptographic algorithm can be carried out in different ways, as indicated by the different routines 315-353 in Fig. 3.

Subsequently, in step B20, the cryptographic processing is executed, in the preferred case by using the DES algorithm in routine 360 in Fig. 3, depending on the desired cryptographic function and key as stated above.

Subsequently, in step B22 (program routine 370 in Fig. 6), the result of the cryptographic processing in step B20 is put together the preferred way according to the function requested, after which the result is sent back to the control computer (PC) 180 in step B24. Subsequently, in step B26, the IC card returns to an idle position awaiting new instructions.

Although the invention has been described above by way of example with reference to an embodiment thereof, it will be appreciated that various modifications and changes can be made within the scope of the invention, which is defined in the appended claims. For example, the design of both the transaction station as a whole and the IC card according to the invention can vary depending on the application in question. Although in the above embodiment, the invention has been described in connection with cash withdrawals from an ATM, it will be appreciated that the invention can also be utilised for carrying out

other types of financial transactions through the central computer. Moreover, the user interface can comprise other types of members than the ones described above. For example, the user interface can comprise a PC with a keyboard, a mouse, and a monitor or the like. The communication between the central computer and the transaction station according to the invention can take place over different types of communication networks. Although it is preferred that the IC card according to the invention is arranged out of reach of the user, preferably in a safety cabinet, it can also be arranged in such a way that it is both accessible to the user and unprotected, since the keys are stored in such a way that they still cannot be accessed by unauthorised individuals.

CLAIMS

1. An IC card designed to be essentially stationarily arranged in a card reader in, or adjacent to, a transaction station in order to cryptographically process data which is to be transmitted from the transaction station to a central computer and/or data which is received by the transaction station from a central computer, said IC card being utilised in connection with the serving of several users of said transaction station, which IC card comprises:

means for storing one or more cryptographic keys;

means for receiving input signals to the card;

means for executing one or more cryptographic algorithms utilising one or more of said cryptographic keys depending upon control information received in said input signals to the card; and

means for outputting output signals, comprising results of said execution, from the card.

2. An IC card according to claim 1, wherein said cryptographic keys comprise one or more master keys utilised in connection with encrypted transmission of other cryptographic keys, such as session keys and authentication keys, from the central computer to said IC card, or alternatively from the IC card to the central computer.

3. An IC card according to claim 1 or 2, wherein said cryptographic keys comprise one or more session keys utilised in connection with encryption/decryption of transaction data transmitted between the transaction station and the central computer, in addition to which said cryptographic algorithms comprise one or more algorithms for encrypting/decrypting said transaction data.

4. An IC card according to claim 1, 2, or 3, wherein said cryptographic keys comprise one or more authentica-

tion keys utilised in connection with the authentication of messages between the transaction station and the central computer, in addition to which said cryptographic algorithms comprise one or more algorithms for authenticating said messages.

5. A transaction station, intended to communicate with a central computer and to serve users in connection with the carrying out of desired financial transactions through the central computer, comprising

a user interface for the inputting of data by a user; and

means for cryptographic processing of data which is to be transmitted to/or be received from the central computer;

c h a r a c t e r i s e d in that

said means for cryptographic processing comprise a card reader intended to receive an IC card according to any one of the preceding claims.

6. A transaction station according to claim 5, wherein said card reader is adapted to receive said IC card so that the latter is kept inaccessible to a user.

7. A transaction station according to claim 6, wherein said card reader is arranged in a safety cabinet.

8. A transaction station according to any one of claims 5-7, wherein said user interface comprises means for inputting a user identity; means for inputting a desired financial transaction and means for inputting an access code.

9. A transaction station according to claim 8, wherein said means for inputting a user identity comprise an additional card reader.

10. A transaction station according to any one of claims 5-9, further comprising means for providing control information, including information about the type of cryptographic processing desired as well as the information required therefor, to said IC card, as well as means for receiving said output signals from the IC card.

11. A transaction station according to any one of claims 5-10 in the form of an ATM.

12. A transaction station according to any one of claims 5-10 in the form of a computer terminal unit, such as a personal computer, configured to enable a user thereof to carry out financial transactions through said central computer.

13. Use of an IC card according to any one of claims 1-4 for cryptographic processing of data which is to be transmitted from a transaction station to a central computer and/or data received by the transaction station from a central computer.

14. Use of an IC card according to claim 13, specifically for encrypting PIN codes.

15. Use of a transaction station according to any one of claims 5-12 for communication with a central computer for the purpose of serving several users in connection with the carrying out of desired financial transactions through the central computer.

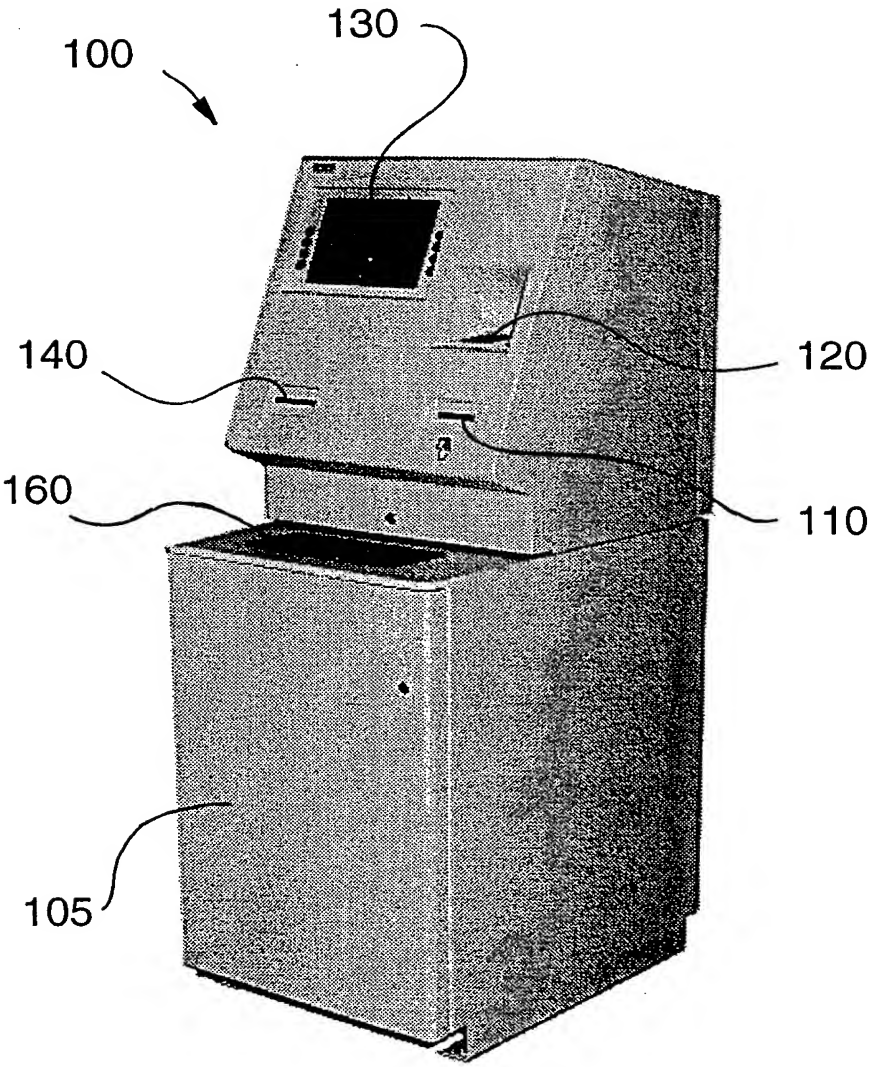


Fig. 1

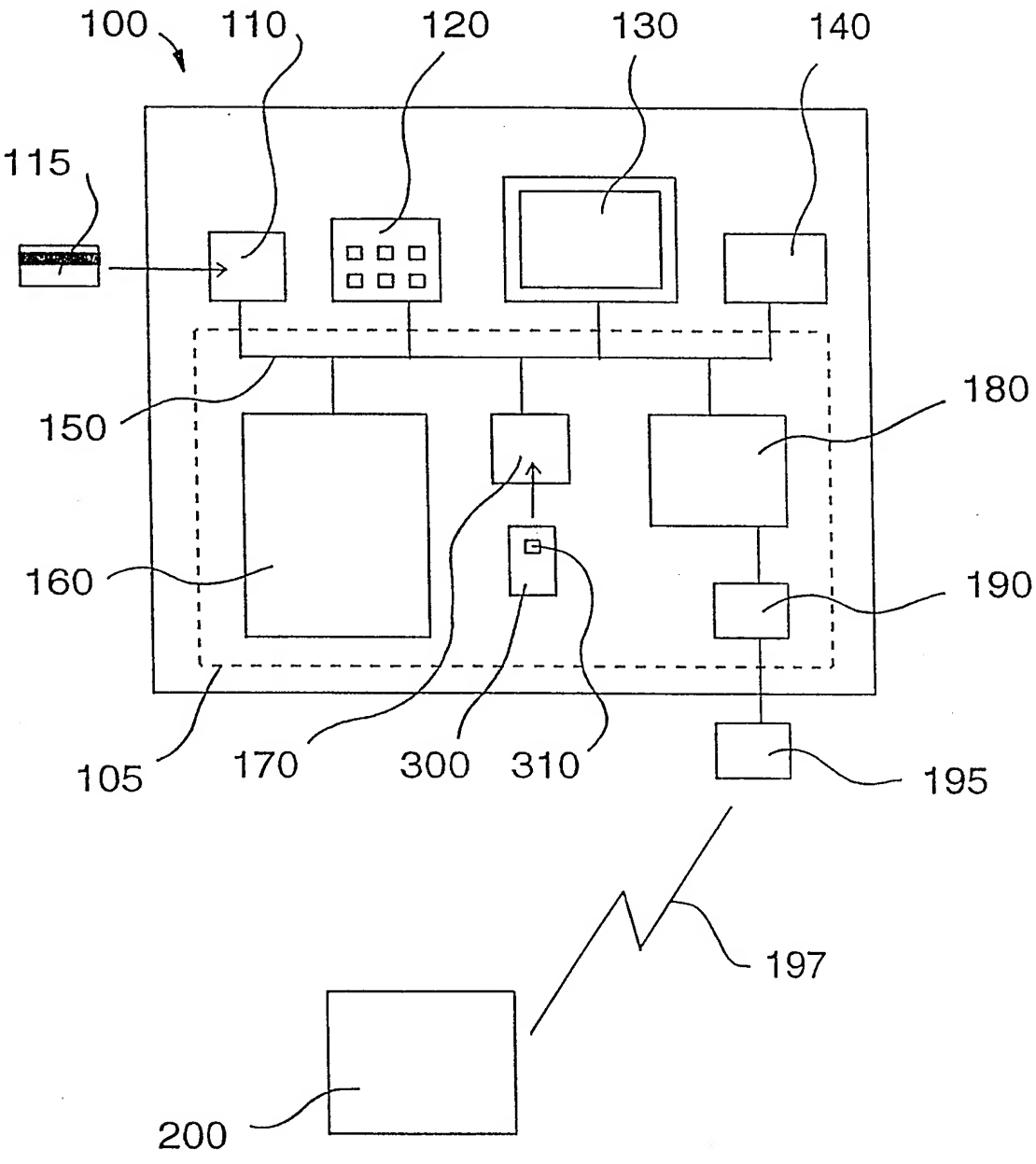

100
110
120
130
140
115
150
180
160
190
105
170
300
310
195
197
200

Fig. 2

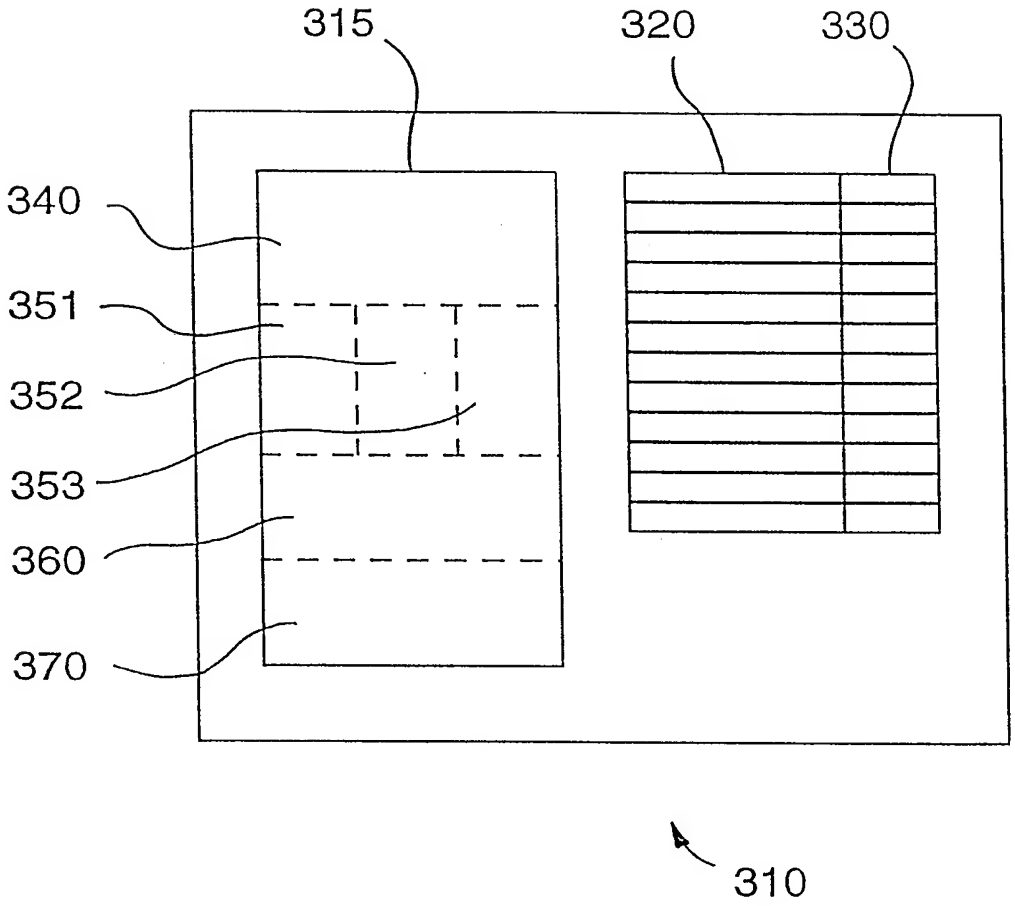


Fig. 3

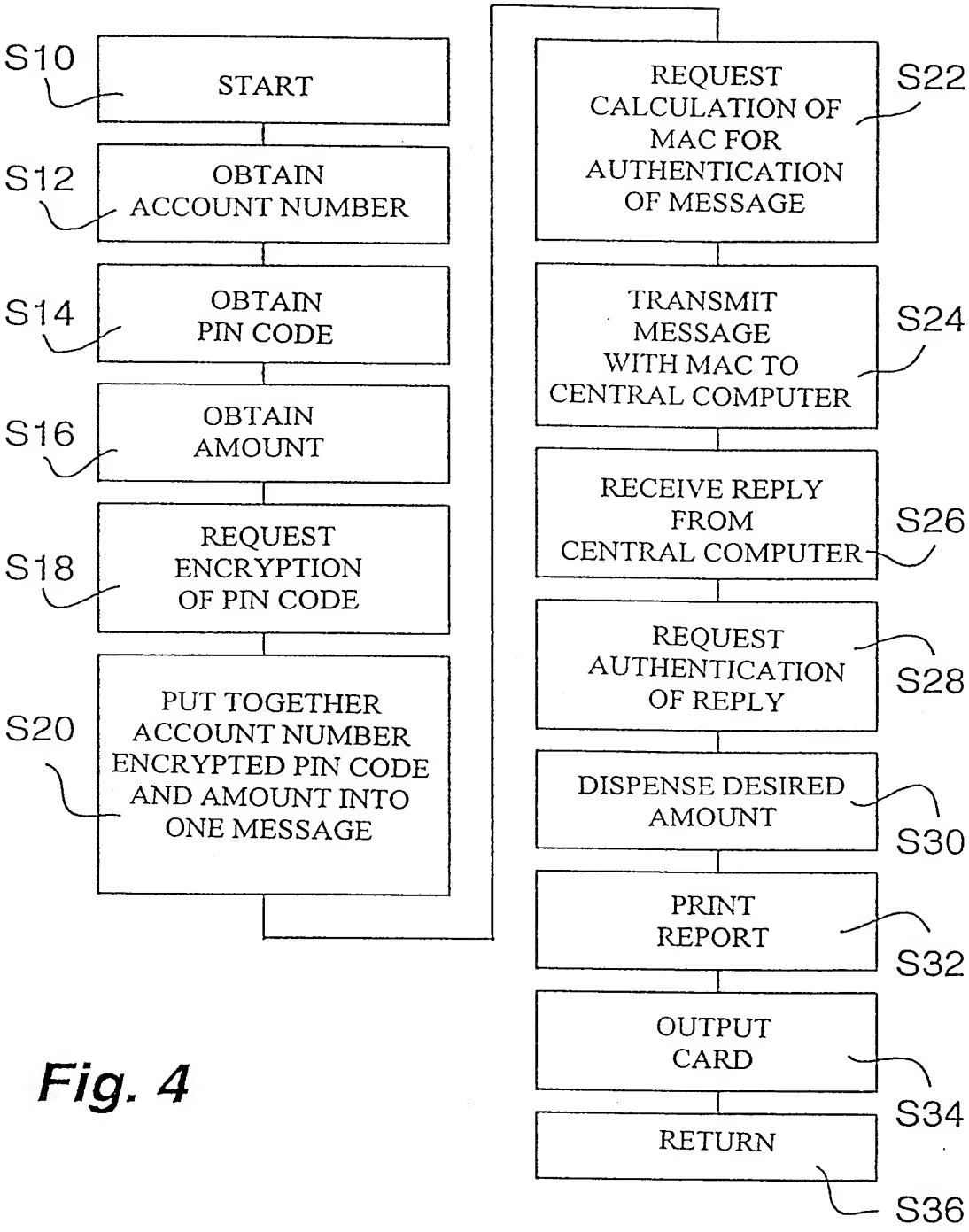
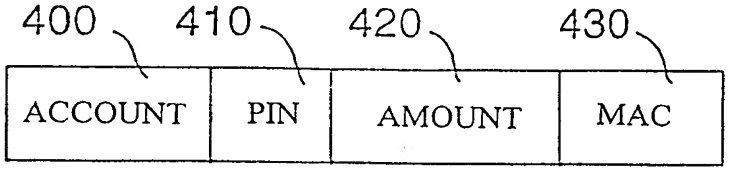

S10
START
S12
OBTAIN ACCOUNT NUMBER
S14
OBTAIN PIN CODE
S16
OBTAIN AMOUNT
S18
REQUEST ENCRYPTION OF PIN CODE
S20
PUT TOGETHER ACCOUNT NUMBER ENCRYPTED PIN CODE AND AMOUNT INTO ONE MESSAGE
S22
REQUEST CALCULATION OF MAC FOR AUTHENTICATION OF MESSAGE
S24
TRANSMIT MESSAGE WITH MAC TO CENTRAL COMPUTER
S26
RECEIVE REPLY FROM CENTRAL COMPUTER
S28
REQUEST AUTHENTICATION OF REPLY
S30
DISPENSE DESIRED AMOUNT
S32
PRINT REPORT
S34
OUTPUT CARD
S36
RETURN

Fig. 4

Fig. 5


400
410
420
430
ACCOUNT
PIN
AMOUNT
MAC

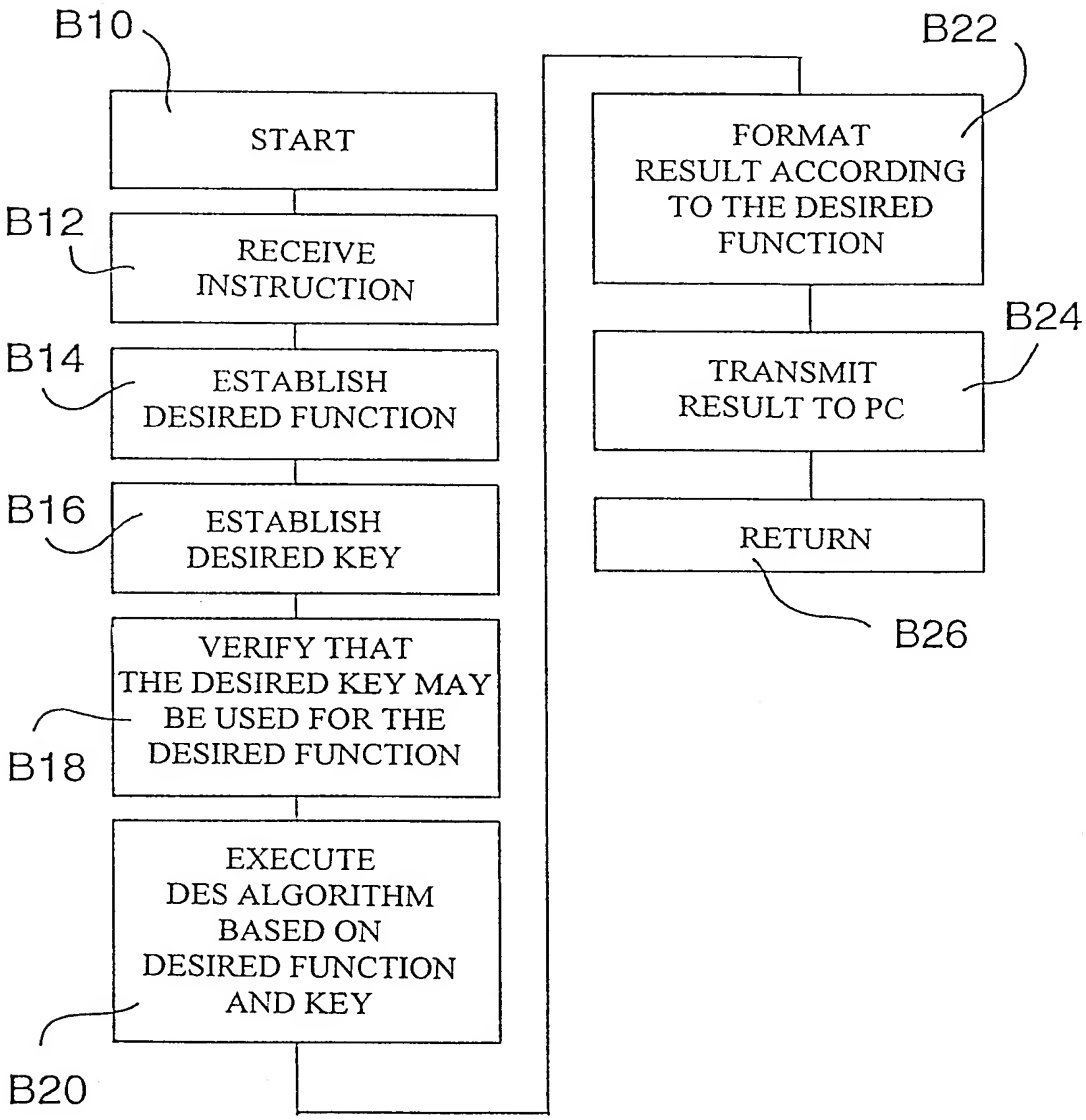

B10
START
B12
RECEIVE INSTRUCTION
B14
ESTABLISH DESIRED FUNCTION
B16
ESTABLISH DESIRED KEY
B18
VERIFY THAT THE DESIRED KEY MAY BE USED FOR THE DESIRED FUNCTION
B20
EXECUTE DES ALGORITHM BASED ON DESIRED FUNCTION AND KEY
B22
FORMAT RESULT ACCORDING TO THE DESIRED FUNCTION
B24
TRANSMIT RESULT TO PC
RETURN
B26

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 98/01019

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G07F 7/10
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04K, G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5448638 A (WILLIAM S. JOHNSON ET AL), 5 Sept 1995 (05.09.95), column 2, line 35 - line 44 --	1-15
A	EP 0138320 A2 (VISA U.S.A. INC.), 24 April 1985 (24.04.85), abstract --	1-15
A	US 5148481 A (DENNIS G. ABRAHAM ET AL), 15 Sept 1992 (15.09.92), abstract --	1-15
A	EP 0151491 A2 (KABUSHIKI KAISHA TOSHIBA), 14 August 1985 (14.08.85), page 3, line 28 - line 30 --	1-15

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 December 1998	02 -12- 1998
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Bengt Romedahl Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 98/01019

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5572696 A (MASAYUKI SONOBE), 5 November 1996 (05.11.96), abstract -- --------	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

03/11/98

International application No.
PCT/SE 98/01019

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5448638 A	05/09/95	US 5384850 A	24/01/95
		US 5228084 A	13/07/93
EP 0138320 A2	24/04/85	SE 0138320 T3	
		JP 60061863 A	09/04/85
US 5148481 A	15/09/92	CA 2026739 A,C	07/04/91
		EP 0421409 A	10/04/91
		JP 3237551 A	23/10/91
		US 5048085 A	10/09/91
EP 0151491 A2	14/08/85	EP 0219879 A,B	29/04/87
		EP 0219880 A,B	29/04/87
		EP 0219881 A,B	29/04/87
		JP 60167044 A	30/08/85
		US 4748557 A	31/05/88
		US 4757543 A	12/07/88
		US 4771460 A	13/09/88
		JP 60167045 A	30/08/85
		JP 60167046 A	30/08/85
US 5572696 A	05/11/96	EP 0544528 A	02/06/93
		JP 5151091 A	18/06/93
		KR 9706999 B	01/05/97